Falta de control de intentos de autenticación en la página de login.

Resumen técnico

El *endpoint* /login de la aplicación web no implementa un mecanismo de limitación de intentos de autenticación fallidos. Esto permite a un atacante realizar un número ilimitado de intentos de contraseña en un corto período de tiempo, lo que expone la aplicación a ataques de fuerza bruta.

Evidencia técnica

Se descubrió la vulnerabilidad utilizando la herramienta

Burp Suite Professional. Se interceptó una solicitud de login con credenciales inválidas y se envió al módulo Intruder. Se configuró un

payload de tipo *sniper* con un diccionario de contraseñas. Se observó que el servidor respondía consistentemente con un código de estado HTTP 200 en cada intento, sin variar la respuesta o introducir retrasos, lo que confirma la ausencia de un bloqueo de intentos.

Impacto potencial

Un atacante podría automatizar un ataque de fuerza bruta para adivinar las credenciales de cualquier usuario, incluyendo las de administradores, comprometiendo la cuenta. El atacante podría obtener acceso no autorizado al sistema y a datos sensibles.

Recomendación técnica

Se recomienda implementar un control de limitación de intentos para mitigar el riesgo de ataques de fuerza bruta. Las siguientes acciones deben ser consideradas:

1. **Bloqueo de cuentas:** Después de un número predefinido de intentos fallidos (ej. 5 intentos), la cuenta de usuario debe ser bloqueada temporalmente.
2. **Retrasos progresivos:** Aumentar el tiempo de espera entre cada intento de autenticación fallido para dificultar la automatización.
3. **CAPTCHA:** Implementar un CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) después de un número específico de intentos fallidos para diferenciar entre un usuario humano y un *script* automatizado.
4. **Bloqueo de IP:** Considerar el bloqueo temporal de la dirección IP de origen después de un número elevado de intentos fallidos para prevenir ataques generalizados